Law 22/2023 of 20 February on the protection of whistleblowers

Corporate Compliance

On 21 February, Law 2/2023, of 20 February, regulating the protection of persons who report regulatory infringements and the fight against corruption, was published in the Official State Gazette. It transposes Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019, known as the "Whistleblowing Directive".

The law will enter into force on 13 March and **companies will have three months** from its entry into force **to adapt their systems** to the new regulation or to implement it, i.e. until **13 June 2023**. As an exception, **companies with fewer than 249 employees have until 1 December 2023.**

The regulation obliges companies with 50 or more workers to have an internal reporting system (previously known as whistleblower channels), as well as a system for the management and protection of whistleblowers, avoiding retaliation against them.

Marimón Abogados has analysed the final text of the Law in order to respond to the essential and most important aspects that affect private sector organisations with a view to a better understanding of its sections, although the scope of the Law also includes Public Administrations.

For further information on the content of this publication:

Lucía Oliveró | **Head of Corporate Compliance**
lolivero@marimon-abogados.com

Anahita Tárrega | **Partner**
tarrega@marimon-abogados.com

What is the purpose of the Law?

The protection against reprisals that may be suffered by natural persons who report certain offences within their work or professional environment through the reporting procedures provided for in the Act.

What reporting procedures are provided for in the Act?

The Law implies the establishment of two reporting systems that can guarantee the confidentiality of the whistleblower: (i) an **internal channel** that is established within the organisations and; (ii) another **external channel** that will be managed by the Independent **Authority for the Protection of Whistleblowers**[1].

Any natural person may report to the Independent Whistleblower Protection Authority the commission of any acts or omissions, either directly or following communication through the relevant internal channel.

Who is obliged to comply with the Act?

a) In the **private sector**: (i) companies with 50 or more employees; (ii) all companies within the scope of application of European Union acts and; (iii) political parties, trade unions, employers' associations and foundations.
b) In the **public sector**: (i) General State Administration, regional and provincial administrations; (ii) public bodies and entities linked to or dependent on a public administration; (iii) public law corporations; (iv) public universities; (v) independent administrative authorities, the Bank of Spain and the managing bodies and common services of the Social Security and; (vi) public sector foundations.

What issues may be reported through the channel?

- **Actions or omissions** that may constitute **breaches of European Union law**[2];
- **Actions or omissions** that may **constitute a serious or very serious criminal or administrative offence.**

In order for the information or communication to be subject to special protection**, it must have been made in good faith**; there must be **reasonable grounds for believing** the possible **infringement** to be true; **and** it must fall within the **scope of protection of the Law.**

[1] Within one year of the entry into force of the Law, the Council of Ministers shall approve by Royal Decree, at the joint proposal of the Ministries of Justice and Finance and Public Administration, the Statute of the Independent Authority for the Protection of Informants (AAI), which shall establish the appropriate provisions on organisation, structure, operation, as well as all the aspects that are necessary for the fulfilment of the functions assigned to it.
[2] The following sectors are covered: public procurement, financial services, products and markets, and prevention of money laundering and terrorist financing, product safety and compliance, transport safety, environmental and climate protection, radiation protection and nuclear safety, food and feed safety, animal health and animal welfare, public health, consumer protection, protection of privacy and personal data, and security of networks and information systems.

Who is protected by the Law?

The Law includes a new nomenclature for the so-called "whistleblower", who is now called "informant".

The Act protects **whistleblowers working in the private or public sector** who have **obtained information about wrongdoing in an employment or professional context**: (i) employees; (ii) self-employed persons; (iii) shareholders, participants and persons belonging to the administrative, management or supervisory body of a company; (iv) staff of contractors, subcontractors and suppliers; and even (vi) volunteers, trainees and paid or unpaid trainees.

Whistleblower protection measures

The whistleblower shall be protected against retaliatory measures for a period of two years.

Where the **whistleblower has demonstrated that he has suffered prejudice, it shall be presumed that the prejudice was caused by retaliation, and it shall be for the person who has taken the injurious action to prove that such action was based on justifiable** grounds unrelated to the disclosure.

Acts constituting retaliation shall be null and void and shall give rise to disciplinary action, including damages.

What are the requirements for internal information systems?

We will focus on how whistleblowing **channels are regulated in private sector companies**, which are now called **Internal Information Systems**.

- The **Administrative Body** of the company will be responsible for the implementation of the system, **after consultation with the legal representation of the workers**, and will be responsible for the processing of personal data in accordance with the provisions of the regulations on personal data protection.
- **Guarantee the confidentiality** of the identity of the informant and third parties and of the actions carried out in the management and processing of the same.
- Allow **communications in writing or verbally**, or both. All communication of information (whistleblowing) must be documented, including those made verbally.
- **Integrate the different internal reporting channels** that may be established **within the entity** (such as, for example, channels for the prevention of harassment, prevention of offences or breaches of the code of ethics, etc.);
- Allowing **anonymous communications**;
- Having an **Information System Manager**;
- Having a **policy** that **regulates the operation of the system**, the defence of the whistleblower and is **publicised within the entity**.

- If the company has a **website, the channel should appear on the home page,** in a separate, easily identifiable section.
- Have **a procedure in place for managing the communications received**;

How will communications received through the internal information system be managed?

The Law establishes that a communications **management procedure must be developed and approved by the Governing Body**. The **person in charge of the system will be responsible for its diligent processing**.

In particular, the procedure shall comply with the following minimum content and principles:

- **Identification of the internal information channel or channels** with which they are associated;
- Those who communicate through internal channels shall be **informed, in a clear and accessible manner, of the external information channels** before the competent authorities and, where appropriate, before the institutions, bodies, organs or agencies of the European Union;
- Send an **acknowledgement of receipt** of the communication to the informant within **7 calendar days** of receipt;
- Provide for the **possibility of maintaining communication with the informant** and **requesting additional information** from him/her;
- **Guarantee the informant's right to be informed** of the actions or omissions attributed to him/her and to be heard;
- **Respect the presumption of innocence**;
- Guarantee of **confidentiality**;
- Determining the **maximum duration of the investigation,** which may not exceed **three months**, except in cases of particular complexity, which may be extended for a further three months; and
- **Referral of the information to the Public Prosecutor's Office** immediately when the facts could be indicative of a crime.

The person responsible for the system

The **Administrative Body** shall be **responsible for the appointment of the System Manager** and for his or her dismissal or removal.

Both the **appointment and the dismissal of the System Manager must be notified to the Independent Authority for the Protection of the Informant** within **ten working days**.

The **System Manager shall be a senior manager of the institution**. Where the size of the institution does not justify the above, the position may be filled by a person with other functions, taking care to avoid

potential conflicts of interest. The role of **System Manager may be assumed by the Compliance Officer**.

Can the management of the internal information system be outsourced to a third party?

Yes, the Law allows outsourcing the management as long as the **third party offers guarantees of respect for independence, confidentiality and data protection.**

The external third party that manages the system will be considered a data processor for the purposes of personal data protection legislation.

Register of communications

Obliged entities shall keep a **register of the communications received and the internal investigations** to which they give rise.

This register shall not be public and only at the reasoned request of the competent judicial authority, by means of an order, and within the framework of judicial proceedings and under the guardianship of that authority, may access all or part of the content of the aforementioned register.

Groups of companies

In the case of a group of companies**, the controlling company shall approve a general policy relating to the internal system** and shall ensure the application of its principles **in all the entities comprising it, without prejudice to the autonomy and independence of each company** which, where appropriate, may establish the respective system of corporate governance of the group, and the modifications or adaptations that may be necessary for compliance with the regulations applicable in each case.

The person in charge of the System may be one for the entire group, or one for each member company thereof. The **internal information system may be one for the entire group.**

The **exchange of information between the different System Managers of the group, if any, shall be admissible** for the proper coordination and better performance of their functions.

The Law does not expressly regulate the cases of multinationals with subsidiaries in different countries. Notwithstanding the above, when the international presence is limited to EU countries, companies must ensure that they comply with EU Directive 2019/1937, of 23 October, and the corresponding national transposition regulations in each country.

Data protection

The processing of personal data in the information channels is considered lawful when it is mandatory to have the information system available because it is necessary for the fulfilment of a legal obligation. Processing is also presumed lawful when the system is not mandatory, but a voluntary decision is taken to create one, as it is necessary for the satisfaction of the public interest.

Constituye **una infracción muy grave no tener implantado el sistema o adoptar represalias contra los informantes**, sancionable con multa de 30.001€ a 30.000€ para las personas físicas, y multa de entre 600.001€ y 1.000.000€ para las personas jurídicas.

Se podrán imponer asimismo sanciones accesorias como la amonestación, la prohibición de obtener subvenciones u otros beneficios fiscales durante un plazo de hasta cuatro años, así como la prohibición de contratar con el sector público durante tres años.

Penalty regime

The Law establishes its own system of penalties. It regulates sanctions to be imposed on individuals or companies in the event of failure to comply with obligations in the management and processing of complaints. The Law categorises infringements as very serious, serious and minor, and for each case it determines a period of limitation and penalties.

The **Independent Authority for the Protection of Whistleblowers** has the power to impose penalties.

It is a **very serious offence not to have the system in place or to retaliate against whistleblowers,** punishable by a fine of between €30,001 and €30,000 for natural persons, and a fine of between €600,001 and €1,000,000 for legal persons.

Ancillary sanctions may also be imposed, such as a reprimand, a ban on obtaining subsidies or other tax benefits for up to four years, as well as a ban on contracting with the public sector for three years.

Conclusions

There is no doubt that the publication of this Law represents a new milestone in terms of compliance for all companies with 50 or more employees, which, in addition to complying with the requirements, must promote integration and collaboration between the different internal channels already in place in the company, such as the channel for reporting harassment, prevention of money laundering and personal data protection.

In short, the internal communication systems will oblige companies subject to the Law to adapt their internal systems to the new regulation or to implement them with the aim of improving transparency, encouraging the collaboration of the employees themselves in the tasks of prevention and discovery of irregular actions within an organisation.

For any information on the content of this publication, we have a multidisciplinary team in labour, data protection and compliance matter available to answer any questions that may arise in this regard. Please also contact us if you need this document in another language.

Barcelona

Aribau, 185

08021

Tel.: +34 934 157 575

Madrid

Paseo de Recoletos, 16

28001

Tel.: +34 913 100 456

Seville

Balbino Marrón, 3

Planta 4ª-10

(Edificio Viapol)

41018

Tel.: +34 954 657 896

www.marimon-abogados.com